Internet Protocol Version 6 (IPv6)
An Overview: What is it and Where is it Going

Edward A. Kierman
732-532-3462
Edward.a.kierman@us.army.mil

4 May 2006

Purpose

- Overview of the DoD and Army commitment to IPv6 and the steps that are in process to guide its transition
- Understand the impacts and benefits of IPv6
- Highlight ongoing IPv6 activities being conducted at the Army's Team C4ISR
- Stimulate additional IPv6 collaboration

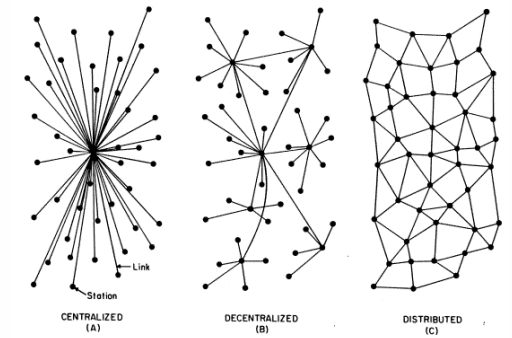
Agenda

- Introduction to IPv6
  - Shortcomings of IPv4
  - Why IPv6
- Technical Overview
  - IPv4 vs. IPv6 comparison
  - Benefits of IPv6
- DoD and Army Perspective
  - DoD / Army Guidance and Governance
  - Army Transition Strategy
  - Return on Investment
  - Transition Challenges
- CE LCMC, SEC Involvement
  - Software Applications
  - IPv6 Center of Excellence
- Beyond DoD

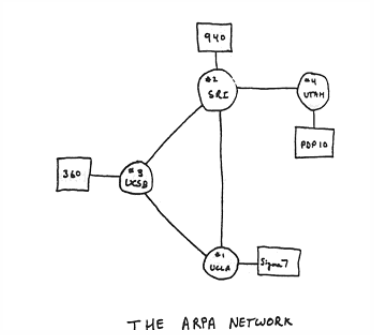
Introduction to IPv6

History

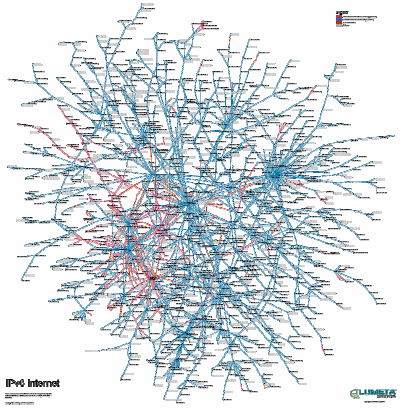
- RAND corporation proposed the basic Internet design (made public in 1964)
- Advanced Research Projects Agency Network (ARPANET) 4 nodes by 1969
- Initially used Network Congestion Protocol (NCP)
  - TCP/IP adopted in 1977 to provide better E2E model than NCP
- Current version of IP (IPv4) has not substantially changed since 1981
  - RFC 791
- IPv6 (RFC 1883) initially released in 1995 to alleviate address shortage, modernize IP protocol, and lower cost by returning Internet to original TCP/IP end-to-end model



The sketch shows Paul Barand's three different network topologies described in his RAND Memorandum, "On Distributed Communications: Introduction to Distributed Communications Network" (1964). The distributed network structure offered the best survivability



By the end of 1969 there are four nodes on the "ARPA NETWORK", UCLA,UCSB, U. of Utah and the Stanford Research Institute (SRI).



The IPv6 Internet backbone today as mapped in Sept 2005 by Lumeta Inc of NJ for the North American IPv6 Task Force IPv6 Deployment Tracking Study

IPv4 Shortcomings – Motivations for IPv6

Infrastructure Upgrade?

- Address Space Limitations: “The prime motivating factor behind upgrade”
  - Xerox, Stanford, MIT and Apple each have a /8 (2^{24}) address block with billions of addresses
  - China only has four /8s for the entire country!
- Cost
  - E2E model to lower the cost of network infrastructure & apps
  - We need a flexible framework to add new capabilities
- Performance
  - “20+ years old and showing its age.”
- Security
  - “Why handle IP Security at L5-L7, when we could standardize it at lower layers?”
- Auto-configuration
  - “We want Plug-N-Play and mobility!”

IPv4 Shortcomings

Address Space "Solutions"

- Classful Subnetting (Old class A,B,C domains)
  - Ex:124.56.72.41 mask 255.255.255.0
- CIDR "Supernetting" (Classless Inter-Domain Routing)
  - Ex: 123.56.72.0/24
- Private Networks (192.168.0.0/16)
- NAT (Network Address Translation) Private:Public translation

While all of these helped, they are only temporary patches

What's Causing IPv4 Troubles?

- Inadequate security feature support
- Deploying peer-to-peer applications complicated by NAT
  - VOIP/SIP
  - Distributed/Cluster computing
  - Direct Video Conferencing
- Explosive Internet adoption in modernizing countries is accelerating address exhaustion
- Workarounds for adding new devices
  - Cellular phones
  - Palm Pilot/Windows CE/Pocket PC
  - Pagers
  - Sensors

- Didn't anticipate the ubiquitous use of IP addresses - The Internet Appliance. "The refrigerator that talks to you."

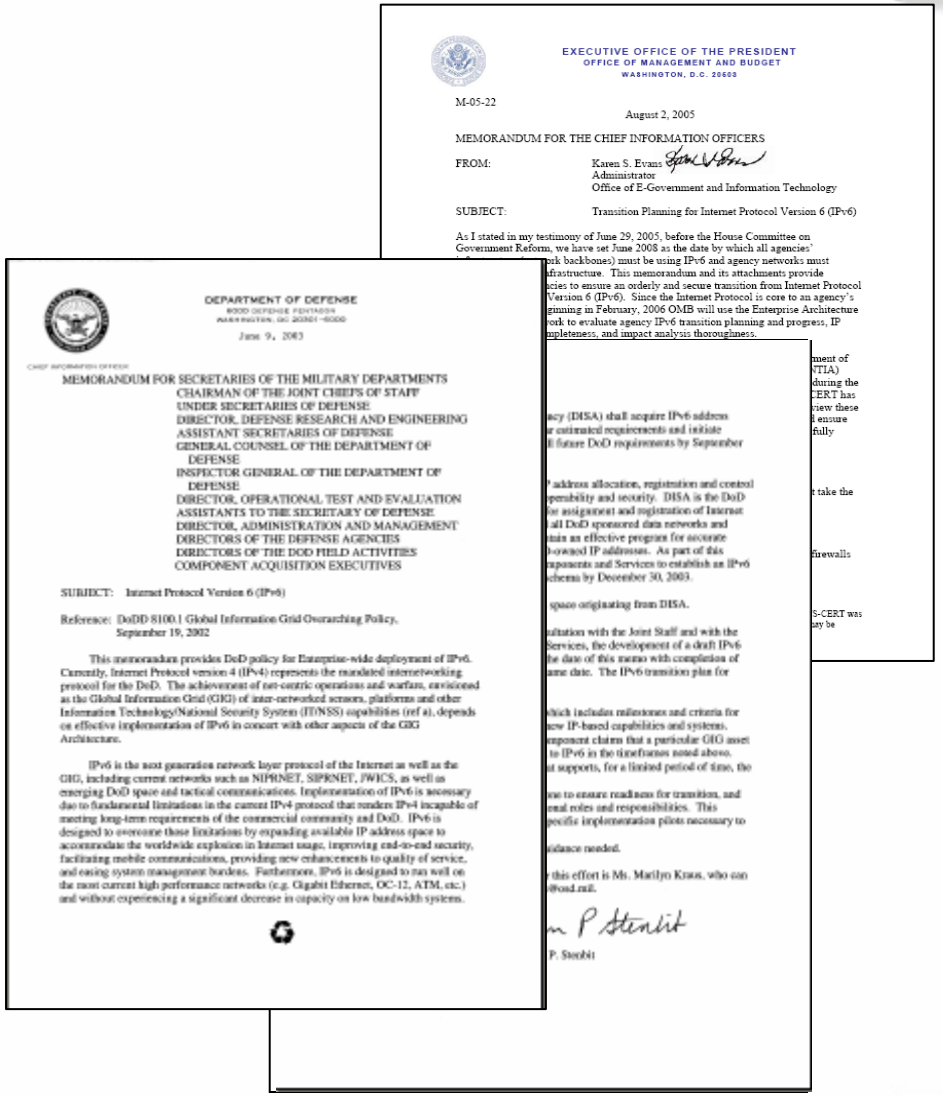
Why IPv6

- Designed primarily to correct shortcomings in IPv4:
  - Efficient routing/header processing
  - Extension headers for future capabilities
  - Improve auto configuration
  - Improve security
  - Improve network management
  - Increase address space
- Use 20 yrs of IPv4 experience to build a flexible framework for next-generation networks
- Keep US infrastructure and IT industry moving forward

Why IPv6

DoD & OMB Mandates

- As of October 2003, all Global Information Grid (GIG) assets being developed, procured or acquired shall be IPv6 capable. Explicitly includes all acquisitions that reach Milestone C after October 1, 2003.
- The GIG will transition to IPv6 operations by FY08; considerable segments will transition between FY05-07
- All Federal infrastructure by June 2008 (OMB)



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies'

DEPARTMENT OF DEFENSE

June 9, 2003

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
COMPONENT ACQUISITION EXECUTIVES

SUBJECT: Internet Protocol Version 6 (IPv6)

Reference: DoDD 8100.1 Global Information Grid Overarching Policy, September 19, 2002

This memorandum provides DoD policy for Enterprise-wide deployment of IPv6. Currently, Internet Protocol version 4 (IPv4) represents the mandated internetworking protocol for the DoD. The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities (ref a), depends on effective implementation of IPv6 in concert with other aspects of the GIG Architecture.

IPv6 is the next generation network layer protocol of the Internet as well as the GIG, including current networks such as NIPRNET, SIPRNET, JWICS, as well as emerging DoD space and tactical communications. Implementation of IPv6 is necessary due to fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting long-term requirements of the commercial community and DoD. IPv6 is designed to overcome these limitations by expanding available IP address space to accommodate the worldwide explosion in Internet usage, improving end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens. Furthermore, IPv6 is designed to run well on the most current high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and without experiencing a significant decrease in capacity on low bandwidth systems.

Technical Overview of IPv6

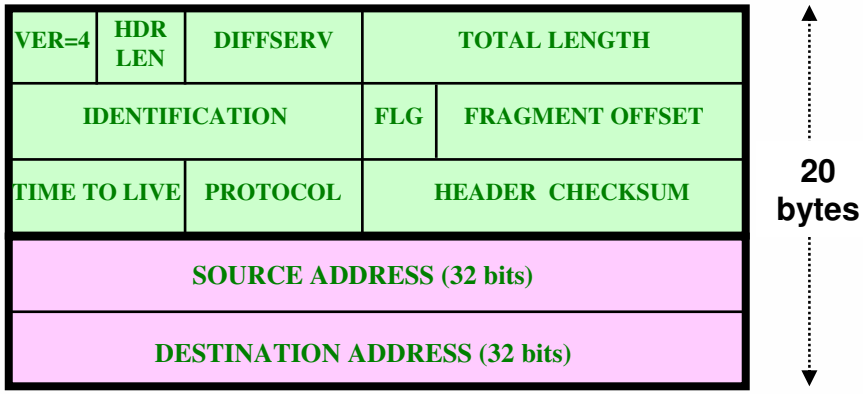
Scale of the Change

IPv6 Spans the Globe!

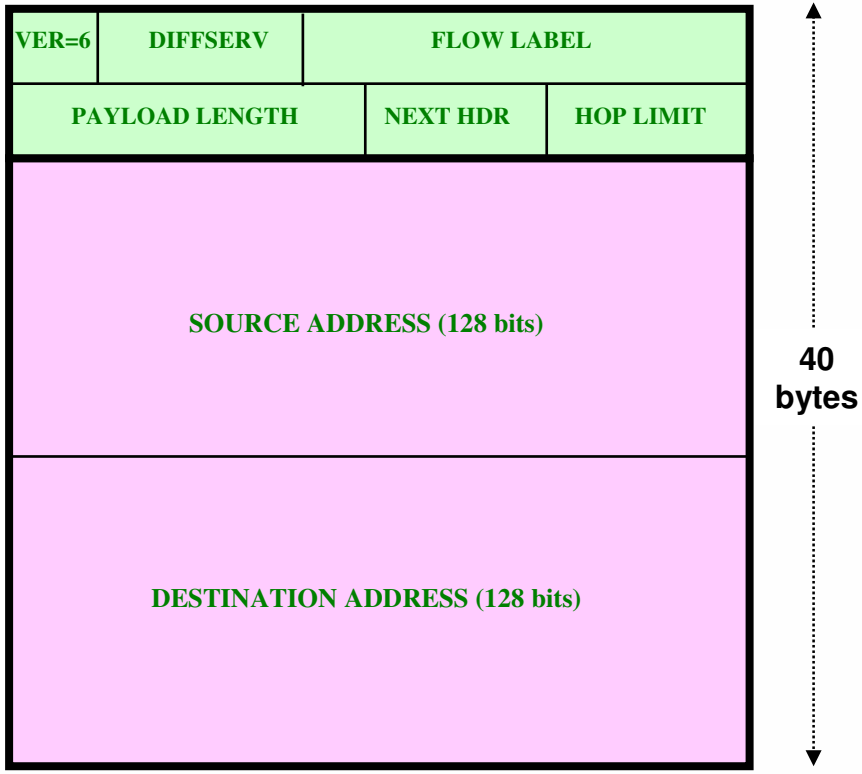
- **IPv6**
  - 128-bit long address
  - 2^128 = 3.4 X 10 ^ 38 addresses
  - Approximately 665 X 10 ^21 addresses per square mile of the earth's surface
  - IP addresses for every grain of sand!
  - Smallest site (soldier/home user?) gets /64 for 2^64 devices!!!
  - Supports proliferation of new customers/devices
  - Promotes cheaper E2E model and reduces infrastructure
- **Compared to IPv4**
  - Only 4 billion total addresses
  - 75% exhausted
  - Scarcity raises cost
  - Most users forced on private address NATs

IPv4 versus IPv6 Header Formats

IPv4 Header



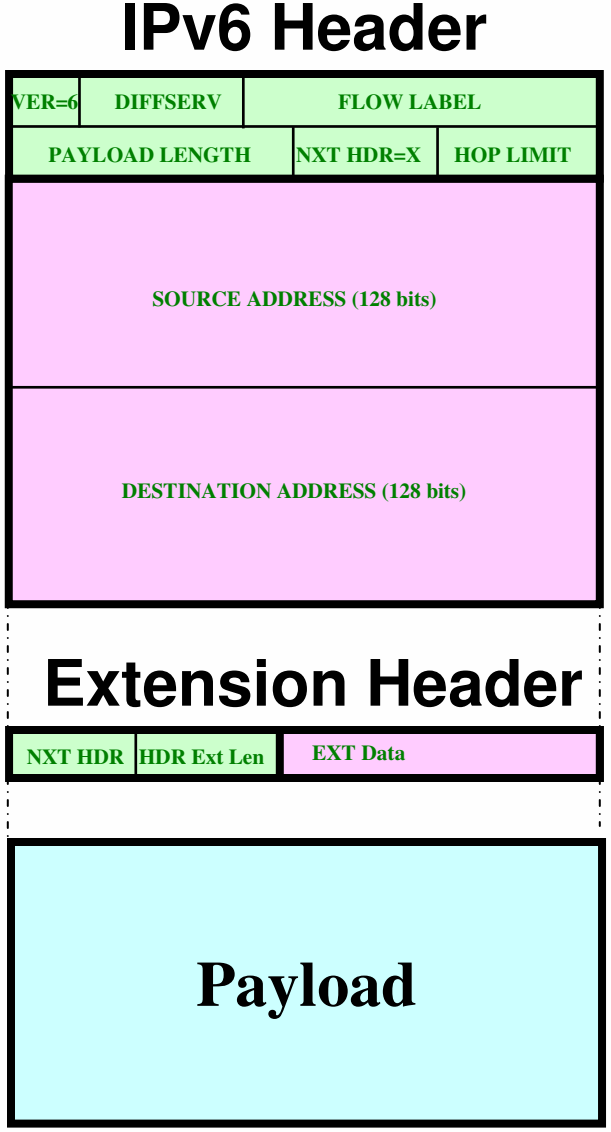
IPv6 Header



IPv6 is not directly backward compatible with IPv4

IPv6 Extension Header Formats

A flexible framework for adding new network services for QOS, Security, etc..



Benefits of IPv6

Core IPv6 Capabilities

- Expanded Address Space ..... Everything Addressable
  - .34 Duodecilion (.34 X 10^{39})
  - Multiple IPv6 Address Per Interface
- Simplified Header ..... Performance Improvement
- Extension Headers and Options ..... Modifiable Protocol
- Authentication and Privacy ..... End-to-End Security
  - Mandatory IPSec
- Auto-configuration ..... Reduced Management Cost
  - Provides Address Mobility
- Source Routing (No Fragmentation) ..... Optimal Data Flows

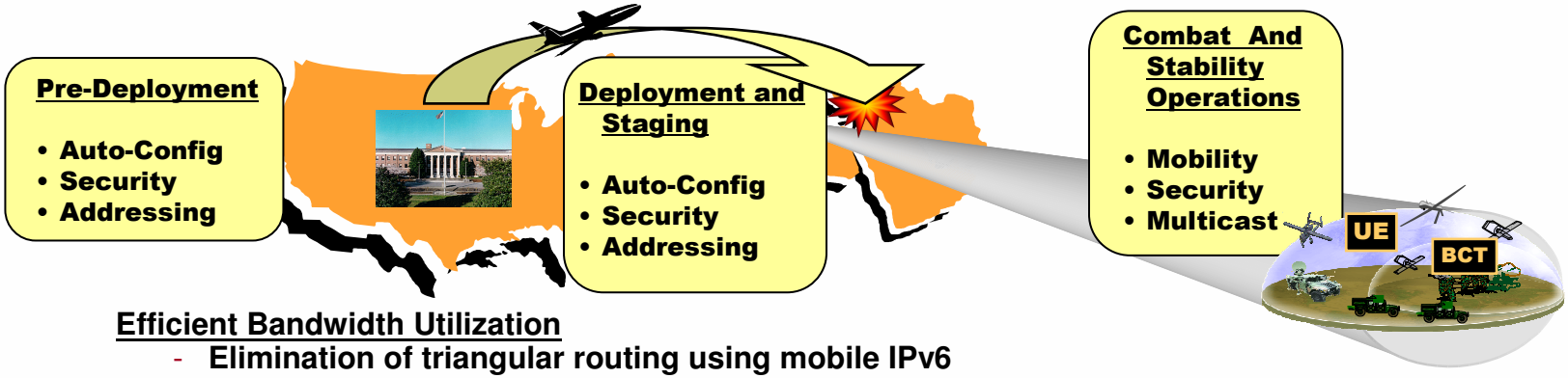
Advanced IPv6 Capabilities

- Advanced Mobility ..... Ad-Hoc Networks (Tactical)
- Flow Labels ..... User Defined Processing
- Quality of Service ..... Priority & Preemption

DoD and Army Perspective

Operational Benefits

IPv6 Benefits Across the Spectrum of Military Operations



Efficient Bandwidth Utilization
- Elimination of triangular routing using mobile IPv6
- Faster packet processing in router (simplified header)

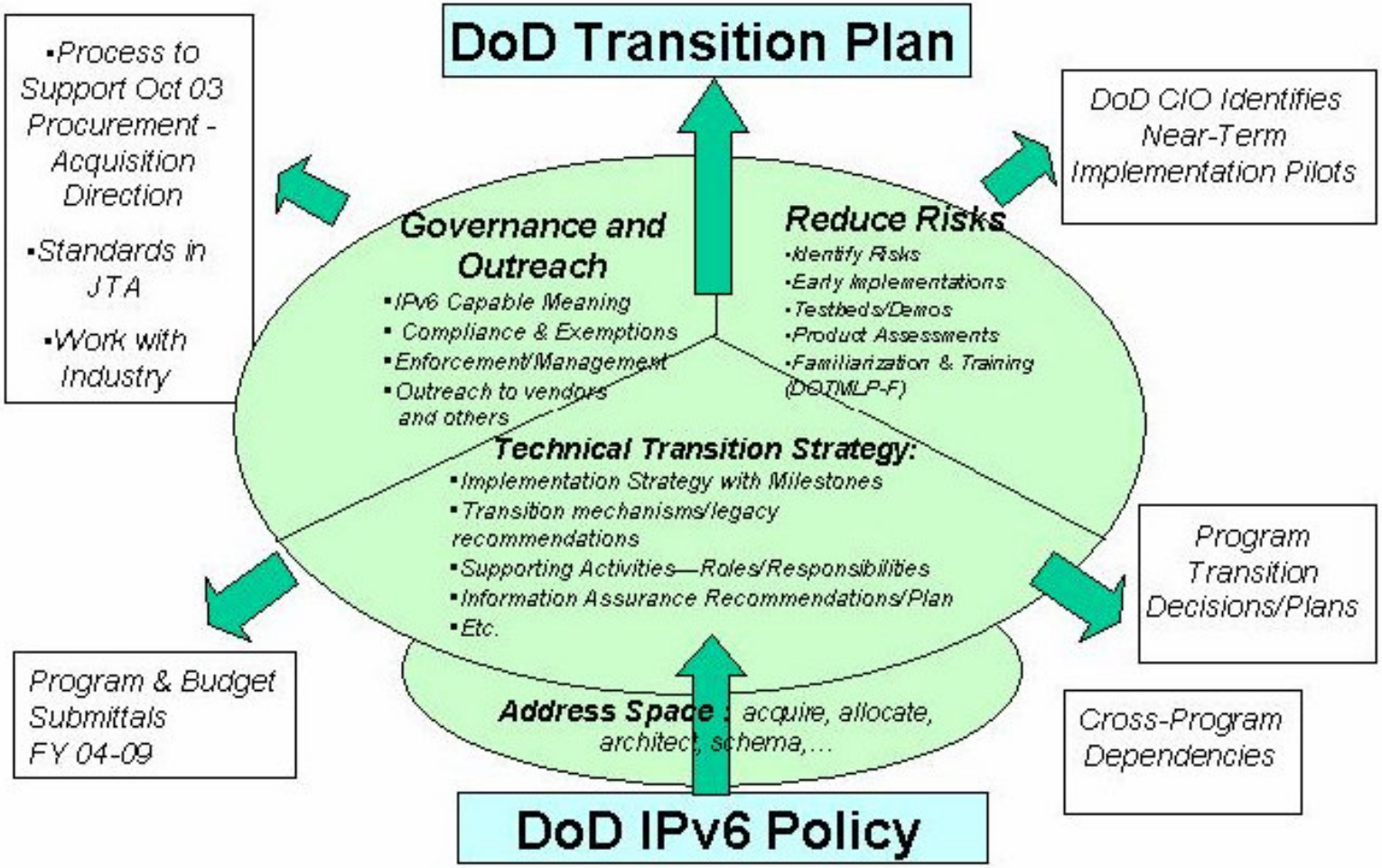
Supports NetCentric Operations and Warfare (Convergence on a single network)
- End-to-end capability
- Larger address space enables every net-enabled device to have dedicated IP address
- Mobility (individual and group)
- Convergence of voice and data on a common carrier

Increases Readiness, Rapid Task Reorganization and OPTEMPO
- Autoconfiguration and renumbering
- Neighbor discovery

Continuous presence (100% availability)
- Mobile IPv6, Network Mobility (NEMO), Multi-homing, Autoconfiguration

Potential to Improved Defense in Depth Security
- Low-level confidentiality, authentication, non-repudiation and integrity
- End-to-end, peer-to-peer security

DoD Guidance and Governance



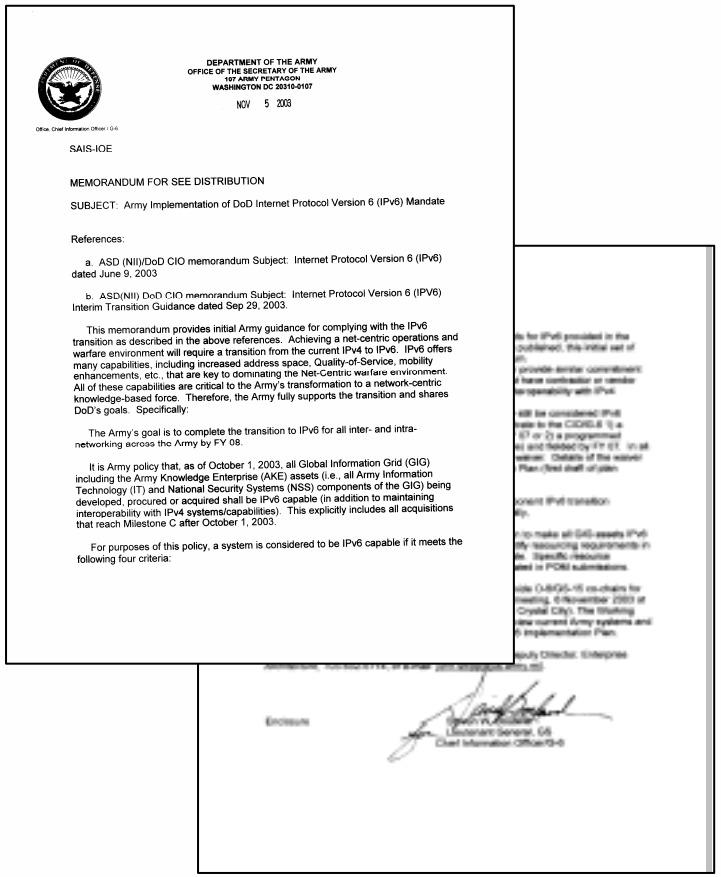
DoD Ground Rules for Implementing IPv6

- **No IPv6 implementations on networks carrying operations traffic within DoD *at this time*.**
- **Components shall develop IPv6 Transition Plans by Apr 2004. Plans shall include:**
  - **IPv6 Implementation Requirements and schedules**
  - **Identify resources for testing, engineering, and pilot implementations**
- **Components will ensure resources needed for overall transition of new and legacy IT by 2008 are included in budget and POM submissions**

Army Guidance and Governance

Proposed Army Technology Transition Office

Army Guidance and Governance



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

NOV 5 2003

Office, Chief Information Officer / G-6

SAIS-IOE

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Implementation of DoD Internet Protocol Version 6 (IPv6) Mandate

References:

a. ASD (NII)/DoD CIO memorandum Subject: Internet Protocol Version 6 (IPv6) dated June 9, 2003

b. ASD(NII) DoD CIO memorandum Subject: Internet Protocol Version 6 (IPV6) Interim Transition Guidance dated Sep 29, 2003.

This memorandum provides initial Army guidance for complying with the IPv6 transition as described in the above references. Achieving a net-centric operations and warfare environment will require a transition from the current IPv4 to IPv6. IPv6 offers many capabilities, including increased address space, Quality-of-Service, mobility enhancements, etc., that are key to dominating the Net-Centric warfare environment. All of these capabilities are critical to the Army's transformation to a network-centric knowledge-based force. Therefore, the Army fully supports the transition and shares DoD's goals. Specifically:

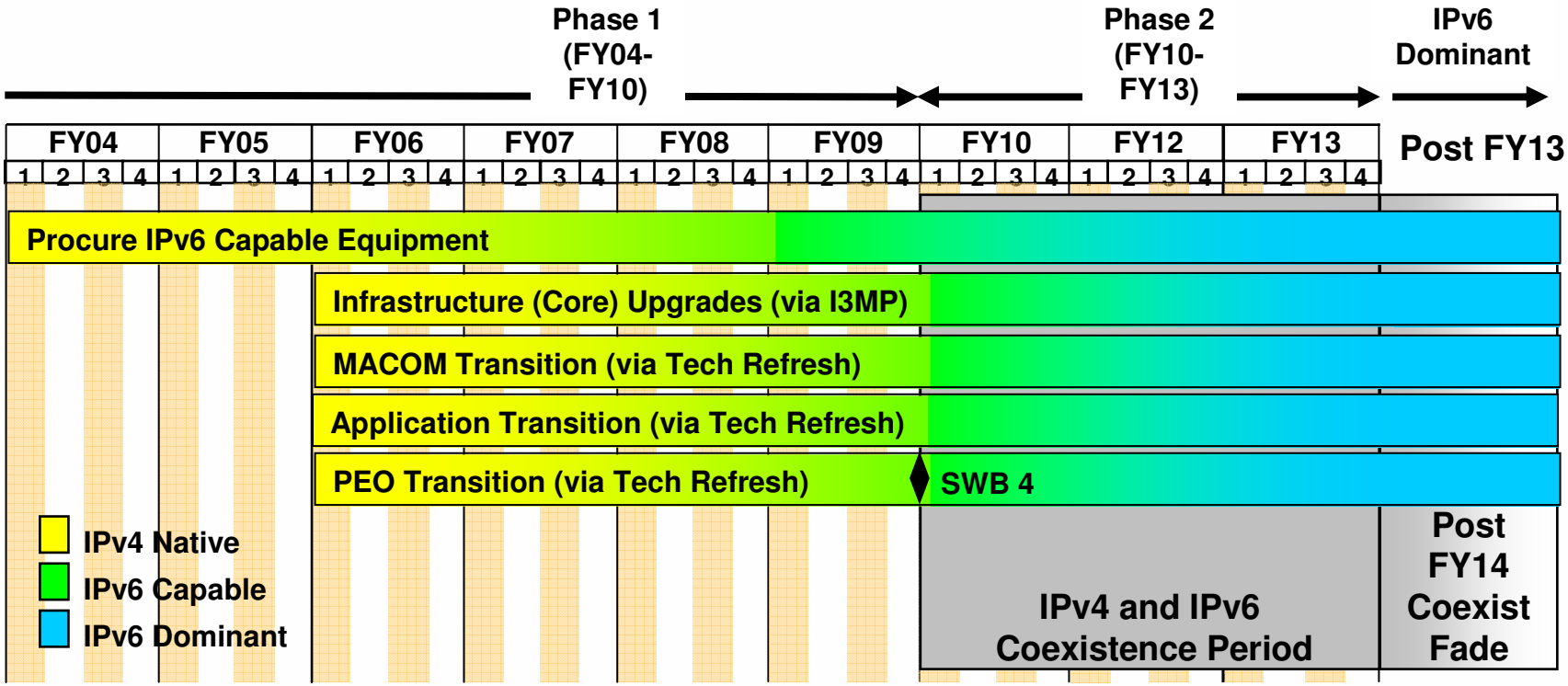
The Army's goal is to complete the transition to IPv6 for all inter- and intra-networking across the Army by FY 08.

It is Army policy that, as of October 1, 2003, all Global Information Grid (GIG) including the Army Knowledge Enterprise (AKE) assets (i.e., all Army Information Technology (IT) and National Security Systems (NSS) components of the GIG) being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities). This explicitly includes all acquisitions that reach Milestone C after October 1, 2003.

For purposes of this policy, a system is considered to be IPv6 capable if it meets the following four criteria:

- Initial Guidance Memo signed by Mr. Borland, 5 Nov 03
  - Reiterates Army and DoD goal of IPv6 transition by FY08
  - Requires PEOs/IMAs/MACOMs to prepare internal IPv6 Implementer's Transition plans for HQDA approval
  - Directs POM Submissions to include IPv6 transition

Army IPv6 Timeline



NOTIONAL -- CONTINGENT ON VALIDATION OF ASSUMPTIONS AND FUTURE TACTICAL NETWORK INTEGRATED PLAN

General IPv6 Network Transition Strategy

- Dual Stack where possible with regular tech refresh
- Use Tunneling (configured and brokered) to provide service through v4-only infrastructure
- Use edge-translation for legacy devices with no upgrade
- Army Enterprise plans: Start with infrastructure, then move to desktop
  - **Routers/switches**
  - **Security Infrastructure**
  - **Management Infrastructure**
  - **Servers (DNS, Office Apps, WWW, NTP, etc…)**
  - **Desktop OS**
  - **Applications**
- Insert advanced IPv6 features and services through updates/service packs

IPv6 Optimization and Return on Investment

- **IPv6 networks that continue to support IPv4 may not achieve many of the netcentric benefits of IPv6**
- Full NetCentric benefits (*return on investment!)* will be achieved when services and applications are run on an **"IPv6 Dominant"** network core and IPv4 transition mechanisms are pushed from the IPv6 network core to the legacy network edge.
- Military systems must go beyond basic dual-stack integration to realize the operational benefits!
- New network services and possible **"Killer Apps"** need basic IPv6 network in place to operate:
  - **Autoconfiguration, auto-reconfiguration**
  - **IPsec "VPN Suite B" (Enhanced cryptography and key exchange)**
  - **Network Mobility (NEMO)**
  - **Mobile IPv6 (MIPv6)**
  - **Secure Neighbor Discovery (SEND)**

DoD Issues and Challenges

- **No Strong Business Case for Transition**
  - Non-competitive in resource battles (no killer apps - yet)
  - Funding shortfalls
  - Best case – future savings, future proof tech, and competitive on a world market
- **Immaturity of Protocol**
  - Industry moving cautiously but accelerating
  - Core infrastructure ready but not edge networks, applications, or security-tools
  - Risk aversion limiting commercial early adopters
- **Dual IP-Layer O&M Costs**
  - Must move to IPv6 dominance quickly
  - Lack of IPv6 trained personnel
- **Security Approvals/Certifications**
  - HAIPE
  - Network Security Best Common Practice for IPv6? Security Policy/Plan?
  - Green light for running operational networks with IPv6???
- **Need for Continued Guidance**
  - Overarching architecture
  - Timetable for integrating IPv6 within the GIG, NCES, and other DOD initiatives
  - Overarching security policy on the "do's and don'ts" that will have significant impacts on transition engineering

Army-Unique Challenges

- Very low bandwidth, high delay & loss in tactical networks
- Highly dynamic networks needed to support on-the-move operations
- Granular mobility of networks: Mobility required among units of action, individual warfighters, vehicles, sensors, and unmanned devices
- Shear volume
  - Many legacy components currently deployed
  - Slow tech refresh for some systems
  - Hundreds of thousands of IP addressable devices
  - Thousands of applications
- Impact of OIF (budget and deployment)

Communications and Electronics Life Cycle Management Center (CE LCMC) Software Engineering Center (SEC)

IPv6 Center of Excellence

- Formation of Team C4ISR (Fort Monmouth) IPv6 Center of Excellence
  - Supporting all phases of IPv6 Transition from research to sustainment
  - Bringing together researchers, developers, T&E community, distribution, and sustainment
- Streamline transition of IPv6-related research into Warfighter systems
- Partnership with private industry, academia, public task forces, and standards bodies
- Prove that Ft Monmouth can act as DoD's

  "One-Stop Shop for IPv6"

IPv6 Center of Excellence

Fort Monmouth Activities:

CE LCMC – SEC

CERDEC – S&TCD, SED

PEO C3T – PM GCC2/CHS, PM TRCS

PEO IEWS

- See: **Army Knowledge Online (AKO) IPv6 Community**
  https://www.us.army.mil/suite/portal/

Other Fort Monmouth Activities:

DISA

- Maintains DoD IT Standards Registry (DISR) & IPv6 Profile
- Coordinates DoD IETF activities
- Leverages Ft Monmouth research activities and facilities
- Coordinates with S&TCD group that represents the Army at IPv6 Standards Working Group (SWG)
- See: **ipv6**.disa.mil/

Current Applications Transition Demo

Purpose

- Demonstrate a viable proof of concept and feasibility to transition a legacy software application
  - Retaining interoperability with IPv4 network functionalities
  - Transparent interoperability with IPv6 networks
  - Demonstrate as many transition mechanisms as possible
  - Demonstrate potential operational scenarios
- Elevate workforce's awareness on DoD/OMB/Army's IPv6 transition mandate
- Train managers and engineers on IPv6 issues/impacts/benefits
- Create a channel for IPv6 knowledge/information exchange within the C4ISR communities

Current Applications Transition Demo

Accomplishments

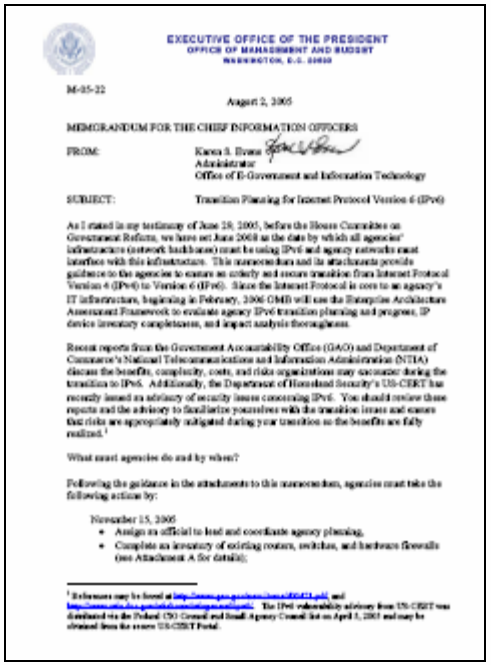
- Developed an Application Layer Gateway (ALG) for the Maneuver Control System-Light (MCS-L) CommServer to enable MCS-L to exchange JVMF messaging in both IPv4 & IPv6 network environments
- Conducted awareness meetings within CE LCMC and Fort Monmouth Community
- Provided separate training to managers and engineers
- Successfully demonstrated the new dual stack MCS-L ALG in February 2006
- Established the Team C4ISR IPv6 web portal on AKO which consists of a forum, news, calendar of events, documents archive, and link to other relevant IPv6 sites

Beyond DoD

OMB IPv6 Mandate

- Memorandum issued 2 August 2005 by Ms. Karen Evans, Administrator, Office of E-Government and Information Technology
- States the following:

"…we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure."



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 19, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of Commerce's National Telecommunications and Information Administration (NTIA) discuss the benefits, complexity, costs, and risks organizations may encounter during the transition to IPv6. Additionally, the Department of Homeland Security's US-CERT has recently issued an advisory of security issues concerning IPv6. You should review these reports and the advisory to familiarize yourselves with the transition issues and ensure that risks are appropriately mitigated during your transition so the benefits are fully realized.[1]

What must agencies do and by when?

Following the guidance in the attachments to this memorandum, agencies must take the following actions by:

November 15, 2005

- Assign an official to lead and coordinate agency planning,
- Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details);

[1] References may be found at http://www.gao.gov/new.items/d05471.pdf and http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/index.html. The IPv6 vulnerability advisory from US-CERT was distributed via the Federal CIO Council and Small Agency Council list on April 5, 2005 and may be obtained from the secure US-CERT Portal.

- Describes four key milestones (dates and activities)
- Addresses
  - Risk Assessment
  - Standards for IPv6 Compliance
  - Impact Analyses – Fiscal, Operational, and Risk Mitigation
  - Guidance from CIO Council Architecture and Infrastructure Committee

World-Wide Government Support for IPv6

Industry and Commercial Support for IPv6

Who supports IPv6?

- *Every Major Equipment Manufacturer!*

Standards Bodies, Associations, and Trade Shows for IPv6

- IETF: Engineers all IPv6 Protocols
  - www.ietf.org
- IPv6 Forum: Promotes IPv6 adoption and interoperability
  - www.ipv6forum.org
- North American IPv6 Task Force (NAv6TF): IPv6 forum chapter in US/Canada – mostly engineering/technical forum for IPv6 subject matter experts
  - www.NAv6TF.org
  - Founded at Fort Monmouth!
- Mid Atlantic IPv6 Task Force (MidAtlanticV6)
  - Local NAv6TF/IPv6Forum chapter in DC to NYC area
  - Fort Monmouth is a founding member!
  - DoD, Federal, University, and Commercial members
  - www.midatlanticv6tf.org/
- US IPv6 Summit Inc: Promotes IPv6 Adoption through popular "summits" (trade shows)
  - www.usipv6.com

Conclusions

- IPv6 technology is mature enough for military networks
- Return on Investment: IPv6 provides new capabilities and a future-proof flexible framework for building netcentric warfare systems
- IPv6 presents engineering challenges and opportunities!
- Transition cost?
  - Regular tech refresh should cover most systems
  - Real cost will be integration, research & development, and training
  - Money savings vs. more powerful networks?
- Team C4ISR IPv6 Center of Excellence can help lead the way!